



高等学校电子与通信类专业“十一五”规划教材

现代编码技术

主编 曾凡鑫
主审 徐澄圻



西安电子科技大学出版社
<http://www.xduph.com>

高等学校电子与通信类专业“十一五”规划教材

现代编码技术

主编 曾凡鑫

主审 徐澄圻

西安电子科技大学出版社

2008

内 容 简 介

现代通信技术正向着大容量、高可靠、强抗干扰、高度机动和业务多元化等方向快速发展,其技术可谓日新月异,本书正是为适应这一通信技术发展的需求而撰写的。本书介绍了最新的编码(序列)构造思想、方法及成果,有许多内容是以往国内同类教材从未涉及的,主要内容包括信息压缩技术,数字传输纠、检错技术,多天线抗衰落空时编码技术和强抗干扰通信系统的序列设计技术等。本书的理论阐述采用“定理一半证明”的叙述模式,并配有大量例题。此外,书末附录给出了学习本课程所需的数学基础知识。

本书内容丰富,取材新颖,难度适中,针对性强,可作为无线通信工程及相关专业的本科教材,也可作为研究生的教学参考书,以及作为工程技术人员研究、开发无线通信技术的参考书。

★ 本书配有电子教案,需要者可登录出版社网站,免费下载。

图书在版编目(CIP)数据

现代编码技术/曾凡鑫主编. —西安:西安电子科技大学出版社,2008.10

高等学校电子与通信类专业“十一五”规划教材

ISBN 978 - 7 - 5606 - 2066 - 4

I. 现… II. 曾… III. 编码—高等学校—教材 IV. O157.4

中国版本图书馆 CIP 数据核字(2008)第 084289 号

策 划 曹 昉

责任编辑 王 瑛 曹 昉

出版发行 西安电子科技大学出版社(西安市太白南路2号)

电 话 (029)88242885 88201467 邮 编 710071

<http://www.xduph.com> E-mail: xdupfxb001@163.com

经 销 新华书店

印刷单位 陕西天意印务有限责任公司

版 次 2008年10月第1版 2008年10月第1次印刷

开 本 787毫米×1092毫米 1/16 印张 20.5

字 数 485千字

印 数 1~4000册

定 价 29.00元

ISBN 978 - 7 - 5606 - 2066 - 4/TN · 0436

XDUP 2358001-1

*** 如有印装问题可调换 ***

本社图书封面为激光防伪覆膜,谨防盗版。

西安电子科技大学出版社
高等学校电子与通信类专业“十一五”规划教材
编审专家委员会名单

主 任：杨 震（南京邮电大学校长、教授）

副主任：张德民（重庆邮电大学通信与信息工程学院副院长、教授）

秦会斌（杭州电子科技大学电子信息学院院长、教授）

通信工程组

组 长：张德民（兼）

成 员：（成员按姓氏笔画排列）

王 晖（深圳大学信息工程学院副院长、教授）

巨永锋（长安大学信息工程学院副院长、教授）

成际镇（南京邮电大学通信与信息工程学院副院长、副教授）

刘顺兰（杭州电子科技大学通信工程学院副院长、教授）

李白萍（西安科技大学通信与信息工程学院副院长、教授）

张邦宁（解放军理工大学通信工程学院卫星系系主任、教授）

张瑞林（浙江理工大学信息电子学院院长、教授）

张常年（北方工业大学信息工程学院院长、教授）

范九伦（西安邮电学院信息与控制系系主任、教授）

姜 兴（桂林电子科技大学信息与通信学院副院长、教授）

姚远程（西南科技大学信息工程学院副院长、教授）

康 健（吉林大学通信工程学院副院长、教授）

葛利嘉（中国人民解放军重庆通信学院军事信息工程系系主任、教授）

电子信息工程组

组 长：秦会斌（兼）

成 员：（成员按姓氏笔画排列）

王 荣（解放军理工大学通信工程学院电信工程系系主任、教授）

朱宁一（解放军理工大学理学院基础电子学系系主任、工程师）

李国民（西安科技大学通信与信息工程学院院长、教授）

李邓化（北京信息工程学院信息与通信工程系系主任、教授）

吴 谨（武汉科技大学信息科学与工程学院电子系系主任、教授）

杨马英（浙江工业大学信息工程学院副院长、教授）

杨瑞霞（河北工业大学信息工程学院院长、教授）

张雪英（太原理工大学信息工程学院副院长、教授）

张 彤（吉林大学电子科学与工程学院副院长、教授）

张焕君（沈阳理工大学信息科学与工程学院副院长、副教授）

陈鹤鸣（南京邮电大学光电学院院长、教授）

周 杰（南京信息工程大学电子与信息工程学院副院长、教授）

欧阳征标（深圳大学电子科学与技术学院副院长、教授）

雷 加（桂林电子科技大学电子工程学院副院长、教授）

项目策划：毛红兵

策 划：曹 昉 寇向宏 杨 英 郭 景

前 言

社会的不断进步强烈地刺激着无线通信技术的快速发展,同时,人们需要通信更快捷、更可靠,业务更加多元化和人性化,也迫使通信技术不断挖掘、研究和开创新技术来适应这一需求。因此,通信技术应最大限度地利用时域、频域、空域和码域等各种资源,尽量提高无线通信的频谱利用率和通信系统的容量,而编码技术正是实现这一目标的关键。

以1948年香农的著名论述《通信的数学理论》发表为标志,编码技术已发展了半个多世纪,当今的编码技术在内容上由传统的分组码、循环码、卷积码、伪随机序列等发展到了Turbo码、LDPC码、空时码、跳频/跳时序列等;在性能上,由与香农理论界限有 $2\sim 3$ dB的差距缩短到了逼近香农理论界限,最好的性能与香农的极限值仅相差 0.0045 dB;在应用上,新技术的应用周期大幅度缩短,分别于20世纪90年代初期和末期发展起来的Turbo码和空时码已成为当今第三代移动通信的主流编码技术。

新的编码技术的发展和应用之迅速是许多从事通信行业的人士始料不及的,工作的需求迫使他们必须了解、掌握这些新编码技术,因此,他们急需一本能综合反映各种新编码技术的发展现状但理论又不过于深奥的入门书籍,本教材正是应这一需求而撰写的。

全书分为8章。第1章为通信与编码概述,简述了通信与编码的关系。第2~8章分为四大模块。第一大模块为信源编码理论,在第2章阐述,主要介绍了传统的无失真编码技术和限失真编码技术。第二大模块为信道编码理论,在第3~6章阐述,其中第3章和第4章分别介绍了传统编码技术——分组码和卷积码,第5章和第6章分别介绍了性能逼近香农理论界限的新编码技术——Turbo码和LDPC码。第三大模块为空时编码技术,在第7章阐述,主要介绍了MIMO通信系统模型、空时分组码、空时网格码、分层空时码和差分空时分组码,这些都是20世纪90年代末发展起来的新编码技术。第四大模块为序列设计原理,在第8章阐述,主要介绍了通信系统与序列的关系、伪随机序列设计、跳频序列设计和跳时序列设计。考虑到编码技术涉及的数学基础较广,并且许多院校又未开设这些基础课,因此,书末附录给出了学习编码技术所必备的数学基础知识,以供读者参考。

本书宜作为通信及相关专业的本科教材,也可以作为研究生教材或学习参考书。本书在内容上覆盖范围宽,内容新,并配有大量例题,但在论述上并不追求推理严谨,许多定理并未证明,这样做的目的是降低初学者的学习难度,让他们把学习的重点放在基础概念和基本方法上,不会因过于深奥的理论而妨碍对新编码技术的迅速掌握。本书努力做到浅显易懂,以期达到教师易教、学生易学的目的。本书对编码、信息序列等多采用矩阵形式进行计算,为统一起见,均用黑斜体表示。

本书在编写过程中,得到了“西安电子科技大学出版社高等学校电子与通信类专业‘十一五’规划教材”评审专家的指导,专家们对本书的撰写提出了宝贵的意见。本书还得到了国家自然科学基金(项目编号:60872164)、重庆市自然科学基金(项目编号:CSTC,2006BB2132)和移动通信信息产业部/重庆市重点实验室开放研究基金(重庆邮电大学)的资助,以及重庆通信学院训练部、教保科和信息工程系领导的大力支持。研究生尹训锋为

本书的初稿做了大量的录入工作。西安电子科技大学出版社的郭景编辑、曹昉编辑对本书的出版给予了帮助和指导。南京邮电大学徐澄圻教授主审了本书，对本书的撰写提出了建设性意见。书末所列参考文献的作者们为本书的撰写提供了丰富的素材。在此，对他们一并表示深深的谢意。

在撰写本书的过程中，虽然作者尽全力确保本书的准确无误，但由于水平所限，也可能存在疏漏之处，祈盼得到广大读者的指正。

作 者

2007 年冬于重庆通信学院

目 录

第 1 章 通信与编码概述	1
习题 1	11
第 2 章 信源编码	12
2.1 无失真信源编码	12
2.1.1 Huffman 编码	12
2.1.2 算术编码	23
2.2 限失真信源编码	30
2.2.1 基本概念	31
2.2.2 离散与连续信源的限失真编码方法	33
2.2.3 最小均方误差准则下的最佳线性预测编码方法	36
2.2.4 最佳变换编码方法	38
习题 2	53
第 3 章 分组码	55
3.1 纠、检错编码的基本概念	55
3.2 线性分组码	59
3.2.1 线性分组码的编码方法	60
3.2.2 线性分组码的译码方法	66
3.3 循环码	70
3.3.1 循环码的编码方法	70
3.3.2 循环码的译码方法	78
3.4 BCH 码	81
3.4.1 BCH 码的定义及最小汉明距离	81
3.4.2 BCH 码的编码方法	82
3.4.3 BCH 码的译码方法	86
习题 3	93
第 4 章 卷积码	95
4.1 卷积码的表示方法	95
4.1.1 卷积码的概念	95
4.1.2 卷积码的多项式表示法	100
4.1.3 卷积码的图形表示法	105
4.1.4 递归卷积码	109
4.2 卷积码的译码方法	111
4.2.1 卷积码的距离概念	111
4.2.2 维特比(Viterbi)译码算法	113
习题 4	121
第 5 章 Turbo 码	123
5.1 Turbo 码的编码原理	123

5.1.1 Turbo 码的典型编码器	123
5.1.2 Turbo 码的典型交织器	129
5.2 Turbo 码的译码原理与性能	134
5.2.1 Turbo 码的一般译码原理	135
5.2.2 Turbo 码的性能与应用	138
习题 5	143
第 6 章 LDPC 码	144
6.1 LDPC 码的概念	145
6.2 二元 LDPC 码的编码方法	150
6.3 LDPC 码的译码方法和性能	158
6.3.1 BF 译码算法	159
6.3.2 LDPC 码的性能与应用	163
习题 6	164
第 7 章 空时编码技术	166
7.1 多输入多输出模型	167
7.2 空时分组码	179
7.2.1 正交空时分组码的编码原理	180
7.2.2 正交空时分组码的译码原理	185
7.2.3 准正交空时分组码	193
7.3 空时网格码	197
7.4 分层空时码	209
7.5 两传输天线差分空时分组码	215
习题 7	223
第 8 章 序列设计原理	225
8.1 通信系统与序列的基本概念	225
8.2 伪随机序列	235
8.2.1 几种相关性能优良的序列	235
8.2.2 反馈移位寄存器序列构造原理	242
8.2.3 m 序列与 M 序列	247
8.2.4 相关性能达到 Welch 下界的序列集	255
8.2.5 已知序列线性复杂度的计算	260
8.2.6 ZCZ 序列	265
8.3 跳频序列	269
8.3.1 至多一次碰撞的跳频序列	270
8.3.2 多项式同余跳频序列	273
8.4 跳时序列	276
习题 8	284
附录 A 数学基础知识	286
附录 B 本原多项式表	312
附录 C 有限域元素表	315
参考文献	317

第 1 章 通信与编码概述

本章将简要介绍通信系统的基本模型、信道模型、编码定理和数字调制的基本原理，这些内容将为后续内容的展开奠定一定的基础。

1. 通信系统的基本模型

自从人类社会诞生以来，人与人之间的交流从未间断过，这种交流或在人与人之间直接进行，或通过机器间接完成。每一次交流，有些人或机器会把某些事物、事物状态或变化的反映(称为信息)表达成一些特定的事务(称为消息)，再通过选定的运载工具(称为信号)传送给选择的人或机器。传送消息的人或机器简称为信源，接收消息的人或机器简称为信宿。在交流过程中，信源希望传送的消息尽量“精练”和适合于在选定的信号载体上传输，这常常需要对信息按某种方式进行重组，这种重组称为信源编码；同时，信源也希望消息在传送过程中具有抗毁性，使消息具有抗毁性的过程称为信道编码。相应地，接收端对接收到的信号首先要进行是否毁坏检验以及恢复处理，这一步通过信道译码来实现，最后再通过信源译码得到信源所传送的消息。通信系统的基本模型如图 1.1 所示，组成部分如下：

信源：消息的发出者。

信宿：消息的接收者。

信源编码器：消息的重组单元。

信道编码器：消息抗毁能力的构建单元。

信道：消息的传输媒介，如电话机之间的电缆、无线电台之间的电磁空间等。

干扰源：毁坏传输信号的各种因素的等价体，可分为自然干扰源和人为干扰源两类。如大气的雷电干扰、电离层的扰动等属于自然干扰；信号的转发干扰等属于人为干扰。

信道译码器：消息的毁坏检验及恢复单元。

信源译码器：消息的还原单元。

发送端：从信源到信道前的各部分的总称。

接收端：从信道后到信宿的各部分的总称。

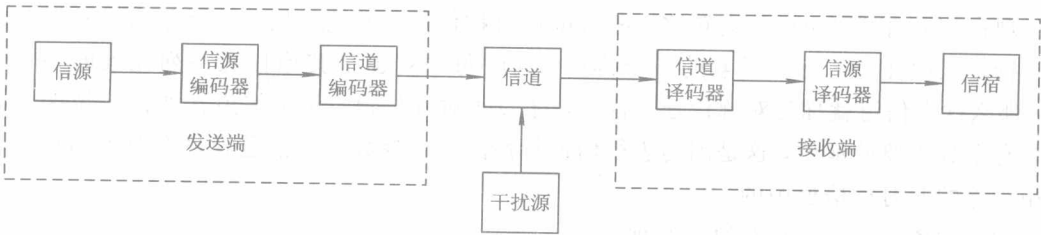


图 1.1 通信系统的基本模型

作为消息的运载体，信号可以表示为随时间连续变化的函数，也可以表示为随时间离

散变化的函数,前者称为模拟信号,后者称为离散信号。传输模拟信号的通信方式称为模拟通信;传输离散信号的通信方式称为数字通信。本书主要讨论数字通信中的编码方法。

2. 信道模型

信道是发送端和接收端之间的连接通道,它可以等效为一个输入端和一个输出端的系统,如图 1.2 所示。

根据信道是否存在干扰,可将其分为无噪信道和有噪信道;根据传输信道是否连续,可将其分为离散信道和模拟信道;根据信道当前输出与先前的输入是否有关,可将其分为有记忆信道和无记忆信道;根据信道参数是否随时间而变化,可将其分为恒参信道和随参信道;此外,信道还可以分为二元信道和多元信道,对称信道和非对称信道,有损信道和无损信道等。上述分类过于简化,实际的信道往往同时具有多种分类的特性。下面介绍几种常用的信道模型。

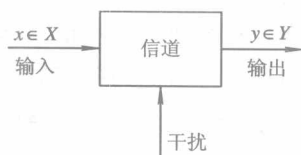


图 1.2 信道简化模型

首先,我们来考虑信道的表示。假设发送端发射的信号都取自字符集:

$$X = \{a_1, a_2, \dots, a_n\}$$

由于信道中存在噪声干扰、传输衰落、传输失真等因素,因此从发送端发出符号 a_i , 在接收端收到的未必是符号 a_i , 甚至于还可能是 X 中不存在的符号。于是可以假设接收端接收的信号都属于符号集:

$$Y = \{b_1, b_2, \dots, b_m\}$$

对给定的信道进行大量的实验后,经统计可以发现:从发送端符号集中发送的符号 a_i 以概率 p_{ij} 转化为接收端符号集中的 b_j 。为方便起见,概率 p_{ij} 常常表示为条件概率的形式,即

$$p_{ij} = p(b_j | a_i) \quad (i = 1, 2, \dots, n; j = 1, 2, \dots, m)$$

这样,用符号转移概率 p_{ij} 就可以充分描述信道特性。为方便起见,引入信道转移矩阵 $\mathbf{P}$, 即

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nm} \end{bmatrix}$$

该矩阵的第 i 行表示字符 a_i 分别转化为 $b_1, b_2, \dots, b_m$ 所对应的概率。

现在,我们可以通过信道转移矩阵来解释对称信道的概念。如果一个信道转移矩阵的每一行是其他任意一行的元素的一个排列,同时每一列也是其他任意一列元素的一个排列,那么这个信道就称为对称信道;否则,称为非对称信道。对称信道在通信系统的设计中具有十分重要的地位,这是因为表征信道特性的一个参数——信道容量在对称信道中比在相对等的非对称信道中的大。

常用的离散信道模型有以下几种:

(1) 二元对称信道。在这种信道中, $X=Y=\{0, 1\}$, 并且 $p(1|0)=p(0|1)=p$, 即字符 0 和 1 发生错传的概率相同,信道转移矩阵 $\mathbf{P}$ 为

$$\mathbf{P} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

二元对称信道常常用状态转移图来简化表示,如图 1.3 所示。

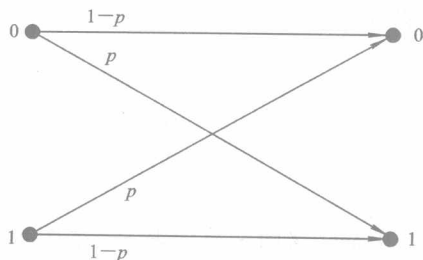


图 1.3 二元对称信道

(2) 二元删除信道。在这种信道中, $X=\{0, 1\}$, $Y=\{0, 1, \omega\}$, Y 中的字符 ω 表示 0 或 1 在传输中发生畸变而在接收端产生的一种发送端字符集中不存在的字符。在一个通信系统中, 字符 0 和 1 分别代表正脉冲和负脉冲, 发送端发送出正脉冲或负脉冲后, 接收端收到的是受到干扰的畸变正脉冲或负脉冲, 当畸变变化比较严重时, 无法识别出是正脉冲还是负脉冲, 这种接收信号就用 ω 来表示。 ω 对接收端是没有意义的, 应被删除。畸变脉冲如图 1.4 所示。

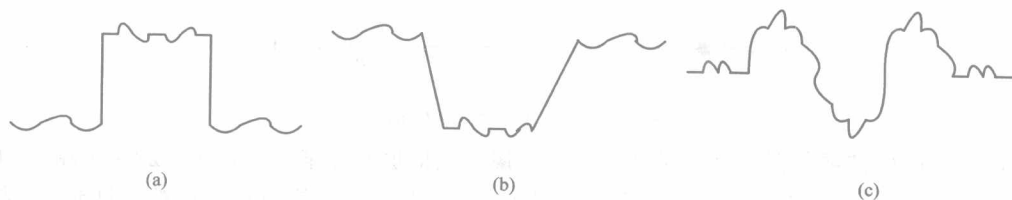


图 1.4 接收端收到的畸变脉冲

(a) 畸变的正脉冲; (b) 畸变的负脉冲; (c) 畸变的脉冲 ω

二元删除信道的信道转移矩阵 $\mathbf{P}$ 为

$$\mathbf{P} = \begin{bmatrix} 1-p & p & 0 \\ 0 & q & 1-q \end{bmatrix}$$

其中, $p(\omega|0)=p$, $p(\omega|1)=q$ 。

二元删除信道常用图 1.5 来表示。

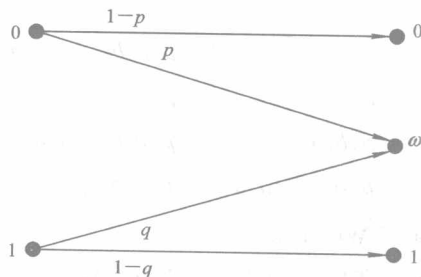


图 1.5 二元删除信道

(3) 多元(N 元)对称信道。在这种信道中, $X=Y=\{0, 1, 2, \dots, N-1\}$,

$$p(i | j) = \begin{cases} 1-p & (i=j) \\ q & (i \neq j) \end{cases}$$

其中, $q = \frac{p}{N-1}$ 。信道转移矩阵 $\mathbf{P}$ 为

$$\mathbf{P} = \begin{bmatrix} 1-p & q & q & \cdots & q \\ q & 1-p & q & \cdots & q \\ \vdots & \vdots & \vdots & & \vdots \\ q & q & q & \cdots & 1-p \end{bmatrix}$$

多元(N 元)对称信道常用状态转移图来简化表示, 如图 1.6 所示。

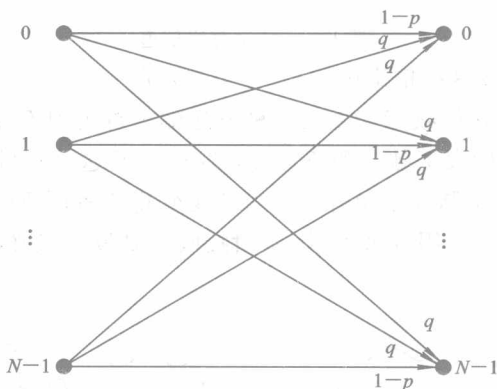


图 1.6 多元(N 元)对称信道

(4) 无记忆扩展信道。 N 维扩展信道可以像前述信道那样来理解, 其差别在于输入和输出信道是一个长度为 N 的字符序列 (视为一个整体), 也相当于信源和信宿被扩展到 N 维空间, 即信源 $X^N = \{(a_{i1}, a_{i2}, \dots, a_{iN}) | a_{ij} \in X\}$, 信宿 $Y^N = \{(b_{j1}, b_{j2}, \dots, b_{jN}) | b_{jk} \in Y\}$ 。例如, $X=\{0, 1\}$, 那么 $X^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$ 。 $\forall \mathbf{x} = (a_{i1}, a_{i2}, \dots, a_{iN}) \in X^N$, $\mathbf{y} = (b_{j1}, b_{j2}, \dots, b_{jN}) \in Y^N$, 字符序列 $\mathbf{x}$ 经信道后转移成 $\mathbf{y}$ 的概率为

$$p(\mathbf{y} | \mathbf{x}) = \prod_{k=1}^N p(b_{jk} | a_{ik}) \quad (1.1.1)$$

由这个转移概率关系不难得到 N 维扩展信道的信道转移矩阵。如 $X=\{a_1, a_2\}$, $Y=\{b_1, b_2\}$, 则 $X^2=\{a_1a_1, a_1a_2, a_2a_1, a_2a_2\}$, $Y^2=\{b_1b_1, b_1b_2, b_2b_1, b_2b_2\}$, 二维扩展信道的信道转移矩阵 $\mathbf{P}$ 为

$$\mathbf{P} = \begin{bmatrix} p(b_1b_1 | a_1a_1) & p(b_1b_2 | a_1a_1) & p(b_2b_1 | a_1a_1) & p(b_2b_2 | a_1a_1) \\ p(b_1b_1 | a_1a_2) & p(b_1b_2 | a_1a_2) & p(b_2b_1 | a_1a_2) & p(b_2b_2 | a_1a_2) \\ p(b_1b_1 | a_2a_1) & p(b_1b_2 | a_2a_1) & p(b_2b_1 | a_2a_1) & p(b_2b_2 | a_2a_1) \\ p(b_1b_1 | a_2a_2) & p(b_1b_2 | a_2a_2) & p(b_2b_1 | a_2a_2) & p(b_2b_2 | a_2a_2) \end{bmatrix} \quad (1.1.2)$$

2) 输入离散、输出连续的 AWGN 信道

AWGN 信道的全称是加性高斯白噪声 (Additive White Gaussian Noise, AWGN) 信道。输入离散、输出连续的 AWGN 信道具有输入信号是离散的、输出信号是连续的、信道

受到的干扰服从高斯分布等特点,是通信中最常用的信道模型之一。图 1.7 是二元输入离散、输出连续的 AWGN 信道简化模型。

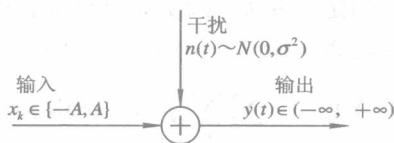


图 1.7 二元输入离散、输出连续的 AWGN 信道简化模型

假设发送的二元离散信号是等概率的,则输入信号的概率密度函数为

$$p(x) = \frac{1}{2} [\delta(x+A) + \delta(x-A)]$$

信道输出为

$$y(t) = x(t) + n(t)$$

发射为 x 、接收为 y 的条件概率密度函数为

$$p(y | x = \pm A) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y \mp A)^2}{2\sigma^2}}$$

式中, $x(t) = \pm A$, $n(t) \sim N(0, \sigma^2)$ 。

3. 编码定理

信源编码的根本目的是提高传输效率,信道编码则以提高传输可靠性为根本目的。读者自然会问,为什么引入信源编码后传输的效率就提高了呢?为什么引入信道编码后就能增加传输可靠性?香农(Shannon)对这两个问题作了明确的回答。

1) 香农第一定理(无失真压缩编码定理)

首先,我们必须了解衡量一种编码传输效率高低的的标准是什么。从通信过程来看,在通信未完成前信宿不知道信源会发送什么消息,信宿收到的消息不确定。例如,在二元对称信道中,设 $p(0) = p(1) = 1/2$ 和 $p(0|1) = 0.2$,那么信宿在一次收到符号 0 时,信源发送符号 0 的可能性只有 80%,还有 20%的可能性是信源发送符号 1。这种不确定性势必造成在信宿必须对接收结果作出判决时产生一定错误的概率。同理,由于事先不可能确定信源会发出什么消息,因而信源也存在不确定性。单一消息的不确定性通过自信息量来度量,但消息的不确定性的统计平均值更能反映问题实质,这种统计平均值度量就是熵(Entropy)。

定义 1.1.1 设离散信源空间 $X = \{a_1, a_2, \dots, a_n\}$, 离散变量 $a_i (i=1, 2, \dots, n)$ 及对应变量的概率分布 $p(X)$ 为

$$\begin{bmatrix} X \\ p(X) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ p(a_1) & p(a_2) & \dots & p(a_n) \end{bmatrix}$$

式中, $\sum_{i=1}^n p(a_i) = 1$ 。

称 $-\lg p(a_i)$ 为离散变量 a_i 的自信息量;称

$$H(X) = - \sum_{i=1}^n p(a_i) \lg p(a_i) \quad (1.1.3a)$$

为信源空间 X 的熵,单位为 bit。

显然, 当 $p(a_i)=0$ 或 $p(a_i)=1$ 时, 离散变量对应的自信息量分别为 $+\infty$ 和 0 , 因为这两种情况中的 a_i 实质上是确定量, 不含有不确定性。出现概率小的离散量的自信息量大, 因为出现概率小, 所以它的不确定性就大。熵实质上是所有离散变量自信息量的平均值。

定义 1.1.2 设有离散空间 $X=\{a_1, a_2, \dots, a_n\}$ 和 $Y=\{b_1, b_2, \dots, b_m\}$, 称

$$H(X|Y) = - \sum_{i=1}^n \sum_{j=1}^m p(a_i, b_j) \lg p(a_i | b_j) \quad (1.1.3b)$$

为条件熵; 称

$$I(X; Y) = \sum_{i=1}^n \sum_{j=1}^m p(a_i, b_j) \lg \frac{p(a_i | b_j)}{p(a_i)} \quad (1.1.3c)$$

为平均互信息量。其中, $p(a_i, b_j)$ 为离散变量 a_i 与 b_j 的联合概率密度, $p(a_i | b_j)$ 为条件概率密度。

在通信中, $I(X; Y)$ 表示平均每收发一对符号信宿得到的信息量。

定义 1.1.3 对信源输出的一列符号序列按一定规则进行变换称为编码, 变换后形成的新序列称为码字, 码字中的每一个元素称为码元, 码元所属符号集称为码符号集, 码字中码元的数量称为码长, 全部码字构成的集合称为码。如果 $q=2$, 则称为二元气码; 如果 $q>2$, 则称为 q 元气码, 这里 q 表示码符号集中元素的个数。

如果在一种码的编译码过程中没有信息损失, 并且该码在理想信道(无噪无信道损失)上传输后能不失真地恢复原消息, 则称该编码为无失真编码; 如果在编译码过程中有控制地损失一些信息, 则称该编码为限失真编码。

限失真编码在通信中是十分重要的, 如一张仅几百兆的光盘能容纳数十小时的视频内容就源于该技术的重要贡献。

定义 1.1.4 设有码 $C=\{c_1, c_2, \dots, c_i, \dots\}$, $p(c_i)=p_i$, 码字 c_i 的长度为 l_i , 称

$$L(C) = \sum_{c_i \in C} p_i l_i \quad (1.1.4)$$

为码 C 的平均码长, 单位为 bit。

定义 1.1.5 设信源符号集为 X , 并有 q 元气码 C , 称

$$\eta = \frac{H(X)}{L(C) \lg q} \quad (1.1.5)$$

为编码效率。

由定义 1.1.5 可知, 对同样的熵, 平均码长越短, 编码效率越高。

引理 1.1.1 (概率匹配原则) 设无记忆信源 $X=\{0, 1, 2, \dots, q-1\}$ 且元素相互独立和等出现概率, 其上有一种码 $C=\{c_i | i=1, 2, \dots, M\}$, c_i 有长度 l_i , 发生概率为 p_i , 若 C 是无损编码且 $L(C)$ 最小, 那么

$$l_i = \log_q \frac{1}{p_i} = - \frac{\lg p_i}{\lg q} \quad (1.1.6)$$

证明 由于 $0, 1, 2, \dots, q-1$ 是独立等概的, 因此每一个这样的元素有自信息量 $-\lg \frac{1}{q} = \lg q$ 。这样, 码 C 中平均每个码字含有的信息量为 $L(C) \lg q$ 。由于是无损编码, 因此 $L(C) \lg q$ 不应当小于 $H(X)$, 又由于 $L(C)$ 最小, 因此

$$L(C) \lg q - H(X) = \sum_{i=1}^M p_i (l_i \lg q + \lg p_i) = 0$$

显然, 当 $l_i \lg q + \lg p_i = 0$ 时上式成立。

概率匹配原则可以这样理解, 因为自信息量小的符号出现概率大, 自信息量大的符号出现概率小, 所以分别用短码和长码表示后, 有利于平均码长的减小。

定理 1.1.1 设离散平稳无记忆信源的熵为 $H(X)$, $X = \{a_1, a_2, \dots, a_n\}$, 那么一定存在一种码 C 使熵和平均码长间满足下列关系:

$$\frac{H(X)}{\lg q} \leq \frac{L(C)}{N} < \frac{H(X)}{\lg q} + \frac{1}{N} \quad (1.1.7)$$

证明 基于信源 X , 构造一个长度为 N 的符号串 $s_i = (r_1, r_2, \dots, r_N)$, $r_i \in X$, 这样的符号串 s_i 形成一个 N 维扩展信源 X^N , 对 N 维扩展信源进行编码, 获得码 $C = \{c_i | i=1, 2, \dots\}$, 每个 c_i 长为 l_i , 发生概率为 p_i 。按概率匹配原则进行编码, 码长应满足:

$$\log_q \frac{1}{p_i} \leq l_i < 1 + \log_q \frac{1}{p_i} \quad (1.1.8)$$

式(1.1.8)两边乘以 p_i 并求和后, 有

$$\sum_{c_i \in C} p_i \log_q \frac{1}{p_i} \leq \sum_{c_i \in C} p_i l_i < \sum_{c_i \in C} p_i + \sum_{c_i \in C} p_i \log_q \frac{1}{p_i} \quad (1.1.9)$$

注意到

$$\sum_{c_i \in C} p_i = 1, \quad \sum_{c_i \in C} p_i \log_q \frac{1}{p_i} = \frac{-\sum_{c_i \in C} p_i \lg p_i}{\lg q} = \frac{H(X^N)}{\lg q}$$

由此可得

$$\frac{H(X^N)}{\lg q} \leq L(C) < 1 + \frac{H(X^N)}{\lg q} \quad (1.1.10)$$

由于是无记忆信源, 故

$$H(X^N) = NH(X) \quad (1.1.11)$$

将式(1.1.11)代入式(1.1.10), 即得式(1.1.7)。

香农第一定理告诉我们, 对于给定的信息熵总能找到一种编码来实现高效传输, 即平均码长最短。

2) 香农第二定理

定义 1.1.6 对离散无记忆信道, 信源和信宿分别为 X 和 Y , $\{p_x\}$ 表示信源 X 的概率分布, 称

$$C_c = \max_{\{p_x\}} I(X; Y) \quad (1.1.12)$$

为信道容量。

信道容量表示信道传送信息的最大能力。对确定的信道, 信道容量是固定不变的, 可以通过改变信源来达到或逼近信道容量。

定义 1.1.7 消息在信道上的传输过程中, 单位时间内传送的实际信息量称为信息传输速率, 记为 R 。

定理 1.1.2 设离散无记忆信道的信道容量为 C_c , $\forall \epsilon > 0$, 总存在一种 $R < C_c$ 的码 C 使接收端恢复消息的误码率 $p_e < \epsilon$ 。同时, 不存在一种 $R > C_c$ 的码 C 使 p_e 任意小。

香农第二定理为在有扰信道上实现可靠传输奠定了理论依据。

顺便指出,在连续 AWGN 信道上,香农信道容量公式为

$$C_c = W \lg\left(1 + \frac{S}{N}\right) \quad (1.1.13)$$

式中: W 表示信道带宽; S 表示信号功率; N 表示噪声功率。

式(1.1.13)是建立扩展频谱通信的基本依据。

3) 香农第三定理

在许多实际情况下进行无失真编码是不必要的,信源可以在信宿恢复消息所需的条件下对消息进行压缩处理,以减小存储或传输的总量。这种压缩方式通常就是去掉消息间的冗余度。要满足信宿恢复消息所需要的条件,就必须在编码时对失真设置一个最大值,称为保真度,记为 D 。保真度越高,即 D 越小,意味着压缩去掉的传输的信源信息量就越少,需要传输更多的信源信息量。很显然,对给定的保真度 D ,信息传输速率 R 不能低于某一个下限值。保真度不同,下限值也不一定相同,即下限值是 D 的函数,称为率失真函数,记为 $R(D)$ 。

定理 1.1.3 对任意给定的保真度 $D \geq 0$,只要码长 N 足够大,一定可以找到一种码 C 使编码后每个符号的信息传输率不小于 $R(D)$,且码的平均失真度不超过 D 。

4. 数字调制的基本原理

通常,来自于信源的信号无论是模拟信号还是数字信号,均不适宜直接在信道上传输,需要先调制后才能进行传输。所谓调制,是指根据调制信号的变化规律去改变载波某些参数的过程。调制具有搬移信号频谱的作用,能够把信号的频谱搬移到理想的位置,从而获得适合于信道传输的信号,大大提高信号传输的有效性和可靠性。调制可以分为模拟调制和数字调制两种,模拟调制的调制信号取值是连续的,数字调制的调制信号取值是离散的。与模拟调制相比,数字调制具有抗噪声能力强、抗信道扰动的鲁棒性高、容易将几种形式的信息融合在一起和安全性好等优点。理想的数字调制技术应能够使通信在低信噪比情况下提供低的误码率,在多径和衰落信道条件下能很好地工作,并且容易实现等。下面主要介绍无线通信中常用的二进制数字调制和 M 进制数字调制,其余的调制(如振幅相位联合键控(APK)、正交振幅调制(QAM)和最小频移键控(MSK)等)不再介绍。

1) 二进制数字调制

二进制数字调制是指调制信号为二进制数字信号的调制方式,在这类调制中,载波的某个参数(如幅度、频率或相位)仅有两种简单的变化状态。二进制数字调制分为幅度键控、频移键控和相移键控三种。

(1) 二进制幅度键控(Binary Amplitude Shift Keying, BASK)。设 x_k 是来自于信源的二进制数字信息 1 和 0,其发生概率分别为 p 和 $1-p$,即

$$x_k = \begin{cases} 1 & (\text{出现概率为 } p) \\ 0 & (\text{出现概率为 } 1-p) \end{cases}$$

则 BASK 信号可以表示为

$$s_{\text{BASK}}(t) = \left[\sum_k x_k g(t - nT_s) \right] \cos(2\pi f_c t) \quad (1.1.14)$$

式中: f_c 为载波频率; $g(t)$ 是一个矩形脉冲; T_s 为持续时间。

式(1.1.14)表明在二进制幅度键控调制中,载波幅度随二进制被调信号序列的变化而改变,如图1.8所示。

(2) 二进制频移键控(Binary Frequency Shift Keying, BFSK)。设 x_k 是来自于信源的二进制数字信息1和0,其发生概率分别为 p 和 $1-p$,则 BFSK 信号可以表示为

$$s_{\text{BFSK}}(t) = \left[\sum_k x_k g(t - nT_s) \right] \cos(2\pi f_1 t) + \left[\sum_k (1 - x_k) g(t - nT_s) \right] \cos(2\pi f_2 t) \quad (1.1.15)$$

式(1.1.15)表明 BFSK 调制信号随被调信号序列在两个载波频率间切换。当 $x_k=1$ 时,使用载波频率 f_1 ;当 $x_k=0$ 时,使用载波频率 f_2 ,如图1.9所示。

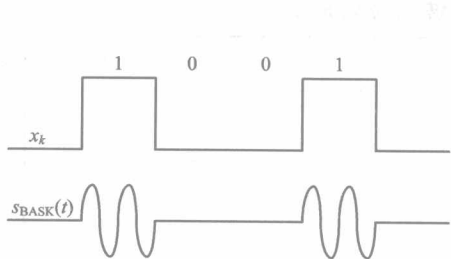


图 1.8 BASK 调制信号示意图

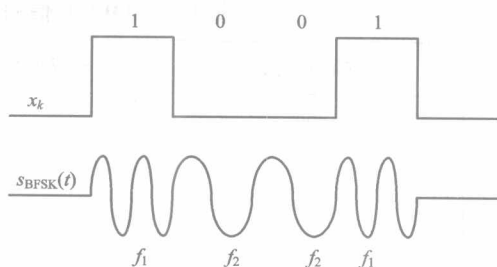


图 1.9 BFSK 调制信号示意图

(3) 二进制相移键控(Binary Phase Shift Keying, BPSK)。设 x_k 是来自于信源的二进制数字信息1和0,其发生概率分别为 p 和 $1-p$,则 BPSK 信号可以表示为

$$s_{\text{BPSK}}(t) = \left[\sum_k (-1)^{x_k} g(t - nT_s) \right] \cos(2\pi f_c t) \quad (1.1.16)$$

在二进制相移键控中,主要使用了下列变换:

$$\begin{aligned} 0 &\rightarrow 1 && (\text{概率为 } p) \\ 1 &\rightarrow -1 && (\text{概率为 } 1-p) \end{aligned}$$

式(1.1.16)表明 BPSK 调制信号随被调信号序列在两个相位相差为 180° 的信号间切换。当 $x_k=1$ 时,载波信号为 $-\cos(2\pi f_c t)$;当 $x_k=0$ 时,载波信号为 $\cos(2\pi f_c t)$,如图1.10所示。

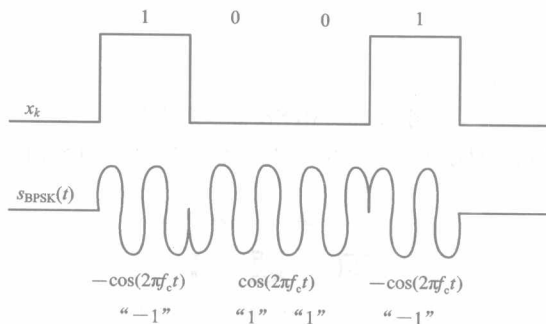


图 1.10 BPSK 调制信号示意图

2) M 进制数字调制

虽然二进制数字调制比较简单,易于实现,但是由于每个码元间隔内可能发送的码元只有两种,而每个码元又只能携带1比特的信息,因此系统的频带利用率不是很高。为了